#15

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): M.J. Coss et al.
Case: 1-1-1
Serial No.: 08/927,382
Filing Date: September 12, 1997
Group: 2787
Examiner: Robert Crockett

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Susan M. Hanlin Date: November 27, 2000

Title: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

---

REPLY BRIEF

RECEIVED
DEC 04 2000
Technology Center 2100

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicants (hereinafter referred to as "appellants") submit this Reply Brief under 37 C.F.R. §1.193(b)(1) in response to the Examiner's Answer mailed on September 25, 2000 relating to the Appeal Brief filed on July 14, 2000 appealing the final rejection of claims 1-26 of the above-identified application.

ARGUMENT

In the Examiner's Answer, the Examiner reiterates that claims 1-26 are unpatentable under 35 U.S.C. §103(a) over Shwed. The Examiner presents further arguments in support of such rejection, attempting to address each of the six independent claims in the present application, i.e., claims 1, 8, 12, 16, 17 and 22, and the respective claims that depend therefrom. Appellants will respectively address below the further arguments offered in the Examiner's Answer with respect to the independent claims, as well as the dependent claims which correspond thereto. Nonetheless, Appellants re-allege herein and incorporate by reference the arguments presented in the Appeal Brief dated July 14, 2000 in their entirety.

(a) Appellants respectfully assert that the claimed security policies of the invention are distinct from the security rules taught by Shwed.

The Examiner contends on page 3 of the Examiner's Answer that "[t]he 'security policies' claimed by Applicants are not distinct from the security rules taught by Shwed." Specifically, with regard to independent claims 1, 8, 12, 17 and 22, the Examiner states that:

> A policy is ordinarily defined as "a definite course or method of action selected from among alternatives." Applicants' specification does not give any special definition to this term. Therefore, one of ordinary skill in the art, at the time the invention was made, would have interpreted the term "security policy" as used in Applicants' claims to be indistinguishable from the term "security rule." This is because a "rule" in this context would have been recognized by one skilled in the art to be "a definite course or method of action selected from among alternatives."

Appellants respectfully disagree. The present specification does indeed specify a difference between the terms "policy" and "rule." For example, at page 5, lines 1-2, it is explained that "[w]ith a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy." Then, at page 5, lines 23-24, it is further explained that "[t]he security policies can be represented by sets of access rules which are represented in tabular form and which are loaded into the firewall by a firewall administrator." Thus, as defined in the present specification, a security policy is a set of rules, i.e., one security policy having multiple rules, and a single firewall may have a plurality of security policies, i.e., several different sets of rules, loaded thereon.

In a given firewall implementing an illustrative embodiment of the claimed invention, a decision module or engine, called a "domain support engine" (DSE), determines which security policy to use for a new network session. In this illustrative embodiment, each new session must be approved by the security policies of the source domain and the destination domain(s). The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. This is explained at page 9, lines 11-17, of the present specification.

Therefore, rule selection in the Shwed system is significantly different than that provided by the claimed invention. As explained above and in further detail in appellants' Appeal Brief, the present invention provides for first selecting a security policy, i.e., rule set, from among a plurality of security policies, i.e., rule sets, and then applying a particular one of the rules from the selected set or policy. By contrast, a firewall in Shwed uses a single rule set as defined by the single packet filter loaded on that firewall. This is clear from the text of Shwed, at column 2, lines 1-4, where it is stated that Shwed "provide[s] a generic packet filter module which is controlled by a set of instructions to implement *a given security policy* at a node . . ." As further explained at column 5, line 52, through column 6, line 6, the set of instructions represent a "filter script which contains *the rules* utilized for the packet filter." Thus, as the express language of Shwed indicates, a single packet filter resides on a single firewall node and implements a single policy which may have multiple rules associated therewith. This is not the same as having a plurality of security policies, with each policy having multiple rules, residing on a firewall node, where at least one security policy is selected and the rules of that security policy are used to validate a packet, as in the present invention.

(b) Appellants respectfully assert that Shwed fails to teach or suggest that a packet filter can apply sets of security rules to packets as in the claimed invention.

The Examiner contends on pages 3-4 of the Examiner's Answer that "Shwed teaches or suggests that his network security system can apply sets of security rules to packets." Whether or not the *overall network security system* of Shwed can apply sets of security rules to packets is not relevant to the claims. What Shwed fails to teach or suggest is a process for selecting at least one of a plurality of security policies as a function of an obtained data item, such as a session key, and using the at least one selected security policy in validating packets of the session, as is defined in the present invention. This selection process may advantageously be performed on a single firewall, as explained above and in the present specification.

By contrast, Shwed is a system for securing inbound and outbound data packet flow in a computer network by employing security rules in appropriately placed packet filters. Each packet filter may handle multiple security rules as a set making it one policy, as mentioned at column 4, lines 23-26. The Shwed system identifies hardware devices controlled by the packet filters as

objects. These objects can be grouped depending on their application, e.g., finance department, research and development department, directors of a company protected by the system. Thus, Shwed permits the control of data flow not only to individual devices on its network, but also to groups of devices.

One example of rule selection in accordance with such grouping ability is discussed in Shwed at column 4, line 58-65. There it is explained that, in accordance with the Shwed system, it is possible to have the chief financial officer, as well as other higher ranking officials of the company, be able to communicate directly with the finance group, but filter out communications from other groups. Further, it is possible to allow e-mail from all groups, but to limit other requests for information to a specified set of computers.

However, this is accomplished by appropriate placement of packet filters and application of a single set of rules within each filter. Each packet filter acts as its own firewall. That is, as explained in Shwed starting at column 7, line 18, a packet is received by a packet filter, compared with a security rule and a determination is made whether or not the packet matches the rule. If the packet matches the rule, a decision may be made to pass or drop the packet based on the requirements of the rule. If the packet doesn't match the rule, then a next rule in the rule set is examined in a similar fashion. Thus, in a manner much like any conventional ordered rule set system, the Shwed system handles group requirements, such as those mentioned in the example above, by simply defining the rules in the *single* rule set in order to implement the group requirements. Again, there is no selection of a security policy from a plurality of security policies and then validation of a packet using the selected security policy, as in the present invention.

Also, on page 3 of the Examiner's Answer, the Examiner states that a "firewall" corresponds to "network hardware supporting one or more packet filters." However, appellants assert that even if network hardware, such as the gateway 122 shown in FIG. 2 of Shwed, contains more than one packet filter (e.g., packet filters 204), each packet filter is dedicated to a connection between the network hardware and the network itself or another network-related device. This is explained at column 3, lines 59-64. Again, each packet filter acts as its own firewall. Thus, whether or not the gateway is termed a "firewall" in Shwed, there is no security policy selection process for a given packet received on a given connection. That is, the packet is subject to the single rule set loaded on the packet filter installed at the connection at which the packet is received.

(c) Appellants respectfully assert that Shwed fails to teach or suggest extraction of data and use of extracted data in a policy selection process as in the claimed invention.

The Examiner contends on pages 4-5 of the Examiner's Answer that "Shwed teaches or suggests that his network security system may extract all types of header data from layered protocol packets for use in matching packets with security rules," and that "Shwed teaches or suggests that packet data which differentiates packets associated with particular network 'sessions' would be useful in rule selection." While these contentions do not appear directly relevant to independent claims 1, 8, 12, 17 and 22, appellants disagree that they support a rejection of claims relating to certain dependent features associated with the present invention. Specifically, the sections of Shwed cited by the Examiner fail to disclose the features of the invention recited in claims 4-7, 18-21 and 23-26. For example, Shwed does not teach that a session key, used in appellant's invention to select a security policy, may include: (i) an Internet protocol (IP) source address, (ii) an IP destination address, (iii) a next-level protocol, (iv) the source port associated with the protocol, and/or (v) the destination port associated with the protocol. Nor does Shwed teach that the next-level protocol may be a transmission control protocol (TCP) or a universal datagram protocol (UDP). Nor does Shwed teach a security policy selecting step comprising the step of determining the network interface at which the request was received and/or to which the request is to be sent. Despite the contention made in the Examiner's Answer, the sections of Shwed cited therein relating to "a data extraction operation" and a "Telnet protocol" do not mention or suggest use of these elements in any security policy selection process.

(d) Appellants respectfully assert that Shwed fails to teach or suggest a rule selection method as in the claimed invention.

The Examiner contends on page 5 of the Examiner's Answer that "Shwed teaches or suggests a rule selection method indistinguishable from Applicants' claimed rule selection method." With respect to this contention, Appellants hereby re-allege and incorporate by reference the arguments presented above in sections (a) and (b) in their entirety. Again, rule selection in the Shwed system is significantly different than that provided by the claimed invention. As explained above, the invention provides for first selecting a rule set or security policy from among a plurality of security

policies, i.e., rule sets, and then applying a rule from the selected set or policy. Shwed simply selects a rule from a single rule set stored on the packet filter and applies it to a packet. Thus, appellants have a 2-layer process while Shwed is a single layer process.

(e) Appellants respectfully assert that Shwed fails to teach or suggest use of source and/or destination network interfaces in a security policy selection process as in the claimed invention.

The Examiner contends on page 5 of the Examiner's Answer that "Shwed teaches or suggests that his security system may be implemented on gateways (firewalls) having multiple hardware interfaces to different networks." The Examiner goes on to conclude that "one of ordinary skill in the art . . . would have recognized that Shwed teaches or suggests how to implement a "firewall" on gateways, routers, and other network equipment by installing packet filters on such equipment and linking a particular packet filter with a particular network hardware interface." Again, while this contention does not appear directly relevant to independent claims 1, 8, 12, 17 and 22, appellants disagree that it supports a rejection of claims relating to certain dependent features associated with the present invention, namely, claims 6, 7, 18-21 and 23-26. Despite the contention made in the Examiner's Answer, the sections of Shwed cited therein relating to where packet filters may be located do not mention or suggest use of source and/or destination network interfaces in any security policy selection process.

(f) Appellants respectfully assert that Shwed fails to teach or suggest that his security system can be used to create multiple independent security areas (domains) and that his security system can administer security domains independently.

The Examiner contends on pages 6-7 of the Examiner's Answer that "Shwed teaches or suggests that his security system can be used to create multiple independent security areas (domains)," and that "Shwed teaches or suggests that his security system can administer security domains independently." With regard to independent claim 16, the Examiner states that column 4, lines 43-67, and FIG. 3 of Shwed suggest "that security areas (domains) can be set up using this security system" based on the motivation that "a hierarchy of privileges would enhance the security of the computer network." Further, the Examiner contends that column 4, lines 27-43 and FIG. 3 of Shwed suggest that the Shwed system could "allow different administrators to configure the

security of different parts of the network, thus allowing more detailed and thorough security." However, any hierarchy of privileges or configuration of different parts of the network that the overall Shwed system may or may not allow is not achieved in the same manner as recited in claim 16 of the present invention.

Independent claim 16 recites the steps of segmenting access rules into a plurality of domains, and administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain. These operations are provided in the context of a firewall in a computer network, as recited in the preamble of claim 16. While the claim defines multiple security policies through the segmentation of access rules into a plurality of domains, claim 16 further defines the additional inventive concept of administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain. This is neither taught nor suggested in Shwed nor believed to be known to those of ordinary skill in the art at the time of the invention. The invention recited in claim 16 thus provides independent rule administration which is a major advantage over Shwed since Shwed would only permit one administrator to control all packet filter rules associated with the firewall.

As described in detail in the Appeal Brief, Shwed's approach to protecting different groups of computers is not accomplished by having separate rule sets loaded in a single firewall, as in the claimed invention, but rather by appropriate placement of packet filters and application of a single set of rules within each filter (column 4, lines 53-58). This only suggests, and appellants suggest necessitates, a single administrator for the entire single rule set. Thus, since there is no suggestion to include multiple security policies in a single firewall device, there can be no suggestion to provide independent administration of respective security policies in a single firewall device, as in the claimed invention.

For at least the reasons mentioned above and in the Appeal Brief dated July 14, 2000, appellants believe that independent claims 1, 8, 12, 16, 17 and 22 are patentable over Shwed and therefore allowable. Regarding dependent claims 2-7, 9-11, 13-15, 18-21 and 23-26, appellants hereby re-allege and incorporate by reference the arguments relating to the above-mentioned independent claims in their entirety. Due at least to the fact that claims 2-7, 9-11, 13-15, 18-21 and 23-26 respectively depend from independent claims 1, 8, 12, 16, 17 and 22, it is believed that such dependent claims are allowable for at least the reasons identified above.

Inasmuch as Shwed and the prior art known to those of ordinary skill in the art at the time of the invention, which the Examiner has characterized as providing certain teachings in the §103(a) rejection of claims 1-26, in fact fail to provide those teachings, this §103(a) rejection is believed to be improper and should be withdrawn.

Respectfully submitted,

William E. Lewis

Date: November 27, 2000

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946